



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

JH

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/925,616	08/09/2001	Simson L. Garfinkel	SGL-001	2959
26161	7590	04/05/2005	EXAMINER	
FISH & RICHARDSON PC 225 FRANKLIN ST BOSTON, MA 02110			SMITHERS, MATTHEW	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 04/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/925,616	GARFINKEL, SIMSON L.	
	Examiner	Art Unit	
	Matthew B Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

**A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
 THE MAILING DATE OF THIS COMMUNICATION.**

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 09 August 2001.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-10, 15-21 and 26-32 is/are rejected.
- 7) Claim(s) 11-14, 22-25 and 33-36 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 09 August 2001 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>11/22/04</u> . | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement filed November 22, 2004 has been placed in the application file and the information referred to therein has been considered as to the merits.

Oath/Declaration

The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because:

It does not state that the person making the oath or declaration has reviewed and understands the contents of the specification, including the claims, as amended by any amendment specifically referred to in the oath or declaration.

More specifically the last phrase "as amended by any amendment specifically referred to in the oath or declaration" is missing from the statement.

Claim Objections

The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. Claim 28 appears to have been numbered as claim 18.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 5, 7-10, 15-16, 18-21, 26-27 and 29-32 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. 5,265,159 granted to Kung.

Regarding claim 1, Kung meets the claimed invention as follows:

"A digital data storage subsystem for storing data in digital form comprising:

a storage medium configured to store digital data;" see element 15.

"a storage control module configured to

i. in response to a storage request requesting storage of digital data, receive the digital data that is to be stored in response to the storage request from a source, encrypt the received digital data using a selected encryption key and enable the encrypted digital data to be stored on the storage medium; and

ii. in response to a retrieval request requesting retrieval of digital data, enable at least one selected portion of the encrypted digital data to be retrieved from the storage medium, decrypt the retrieved encrypted digital data using a selected decryption key, and provide the decrypted digital data to a destination;" see element 16.

and

"a sanitization control module configured to, in response to a sanitization request, make the decryption key unavailable to the storage control module, thereby disabling the storage control module from thereafter decrypting the encrypted digital data stored on the storage medium." see column 3, lines 2-49; column 3, lines 6 to column 4, line 34 and Figure 1.

Regarding claim 2, Kung meets the claimed invention as follows:

"A digital data storage system as defined in claim 1 in which the storage medium is a magnetic medium, in which the encrypted digital data is stored in magnetic form." see column 2, lines 57-59 (. . . hard disk employed as the storage medium 15 . .).

Regarding claim 3, Kung meets the claimed invention as follows:

"A digital data storage system as defined in claim 2 in which the magnetic medium is a disk." see column 2, lines 57-59 (. . . hard disk employed as the storage medium 15 . . .).

Regarding claim 5, Kung meets the claimed invention as follows:

"A digital data storage system as defined in claim 1 in which the storage control module is configured to make use of a symmetric key encryption and decryption methodology in encrypting the digital data and decrypting the encrypted digital data." see column 3, lines 46-49 (In the two way mode . . . encrypted using the random key 21 . . . the key 21 . . . may be used . . . to recover the data . . .)

Regarding claim 7, Kung meets the claimed invention as follows:

"A digital data storage system as defined in claim 1, the digital data storage system further comprising a decryption key store configured to store the decryption key, and the

storage control module is configured to make use of the decryption key stored in the decryption key store in decrypting the encrypted digital data." see column 3, lines 45-62; column 3, lines 6 to column 4, line 34 and Figure 1.

Regarding claim 8, Kung meets the claimed invention as follows:

"A digital data storage system as defined in claim 7 in which the sanitation control module is configured to make the decryption key unavailable; to the storage control module by wiping the decryption key from the decryption key store." see column 3, lines 34-44; column 3, lines 6 to column 4, line 34 and Figure 1.

Regarding claim 9, Kung meets the claimed invention as follows:

"A digital data storage system as defined in claim 8 in which the sanitation control module is configured to wipe the decryption key from the decryption key store by erasing the decryption key store." see column 3, lines 34-44; column 3, lines 6 to column 4, line 34 and Figure 1.

Regarding claim 10, Kung meets the claimed invention as follows:

"A digital data storage system as defined in claim 1, the digital data storage system further comprising a key generator configured to generate the decryption key." see column 3, lines 45-62; column 3, lines 6 to column 4, line 34 and Figure 1.

Claims 15, 16, 18, 19, 20, and 21 are computer program product claims that are substantially equivalent to system claims 1, 5, 7, 8, 9, and 10, respectively. Therefore, claims 15, 16, 18, 19, 20, and 21 are rejected by a similar rationale.

Claims 26, 27, 29, 30, 31 and 32 are method claims that are substantially equivalent to system claims 1, 5, 7, 8, 9, and 10, respectively. Therefore, claims 26, 27, 29, 30, 31 and 32 are rejected by a similar rationale.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. patent 5,265,159 granted to Kung and further in view of U.S. patent 6,414,884 granted to DeFelice et al.

Regarding claim 4, Kung discloses everything claimed as applied above (see claim 1), except, Kung fails to specifically teach the storage medium as an electronic medium. DeFelice discloses a method and apparatus for preventing stored information from unauthorized access whereby the stored information can be on electronic media as well as magnetic storage devices (see column 1, lines 18-23). It would have been obvious to one of ordinary skill in the art at the time of the invention to include DeFelice's apparatus for securing stored information with Kung's secure file erasure system in order for a user to gain the advantage of using the permanently erasure technique on any type of storage medium. The combination shows the type of storage

method does not affect the procedural steps of securely protecting information stored on a particular type of medium.

Claims 6, 17 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. patent 5,265,159 granted to Kung and further in view of U.S. patent 6,414,884 granted to Langford.

Regarding claim 6, Kung discloses everything claimed as applied above (see claim 1), except, Kung fails to specifically teach the storage control module uses an asymmetric key methodology to encrypt/decrypt the data. Langford teaches a system and method for securely deleting data within a storage medium where the storage control module (secure data deleter 200) uses an asymmetric key process to encrypt/decrypt data (see column 5, lines 19-42)(. . . secure data deleter 200 performs deletion processing by reading the desired data to be deleted from the memory 108 and encrypts the data using any suitable encryption key using the encryptor 204. The encryptor 204 may be any suitable encryption algorithm . . . a public key (asymmetric) encryptor employing an RSA encryption or elliptic curve process . . .). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Langford's system for securely deleting data with Kung's secure file erasure system in order to gain an advantage of using a generated public key encryption pair (public key for enciphering, private key for deciphering). A well known advantage of using a public key encryption process is that the public key process provides stronger security over a symmetric key process because access to the enciphering (public) key by others does not enable them to decipher the encrypted information.

Claim 17 is a computer program product claim that is substantially equivalent to system claim 6. Therefore, claim 17 is rejected by a similar rationale.

Claim 28 is a method claim that is substantially equivalent to system claim 6. Therefore, claim 28 is rejected by a similar rationale.

Allowable Subject Matter

Claims 11-14, 22-25 and 33-36 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

With respect to claims 11-14, 22-25 and 33-36 the cited prior art fails to specifically teach a digital data storage subsystem, method and computer program product in which the key generator module is configured to generate the decryption key from two bit patterns provided thereto using a predetermined generation methodology.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Friedman et al (US 6,212,600) disclose a method for sanitizing fixed storage devices.

B. Cromer et al (US 2003/0028765 A1) discloses a system for protecting information from being read by another computing system by encrypting the data structure of a disk.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew T Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Matthew B Smithers
Primary Examiner
Art Unit 2137